DEPARTMENT OF THE ARMY
UNITED STATES ARMY GARRISON VICENZA
UNIT 31401, BOX 41
APO AE 09630

IMEU-VIC-PLIA

18 SEP 2008

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: U.S. Army Garrison Vicenza Policy Memorandum 08-23, Information Systems Users Responsibilities Policy

1. The policy memorandum supersedes U.S. Army Garrison (USAG) Vicenza Policy Memorandum 06-41, Computer User Policy dated 24 February 2006.

2. Reference AR 25-2, Information Assurance, 24 October 2007.

3. This policy applies to all military, Civilians and host nation employees within the United States Army Garrison (USAG) Vicenza and USAG Livorno communities.

4. All government computer **users** within the USAG Vicenza and USAG Livorno will adhere to the following Information Systems (IS) user rules:

a. **COMPUTERS**. All computers will be **left-on** unless otherwise instructed by your Information Assurance Security Officer (IASO), Information Management Officer (IMO), or the Garrison Information Assurance Manager (IAM). At the end of the day, the user will **re-start** the computer and leave it **on** *(do not log back-in)*. All monitors and other peripherals, i.e. printers, facsimiles etc in the area will be **turned-off** for energy conservation. Computers are regular scanned by IASO/IAM for security compliance. Vulnerable computers constitute a threat to the Army network and immediate action must be taken to fix it or disable from the network updated. Most vulnerability found are the results of computers being turn-off or not restarted frequently. If a computer is disabled for non-compliance, users need to submit a work order through the help desk (119) or on-line ticket to https://jazz.anosc-e.5sigcmd.army.mil/arsys/119. This ticket will be send to users local IMO for resolution. Please keep in mind due to other high priorities and limited technical personnel, this action may not be corrected immediately. **RESTART YOUR COMPUTER AND LEAVE ON AT THE END OF THE WORK DAY, WHEN ON LEAVE OR TDY!**

b. **LAPTOPS/NOTEBOOKS**. All laptops and notebooks should remain connected to the network when not on TDY status. This will allow the system to stay up-to-date and virus protected. If the laptop or notebook computers have not been connected to the USAREUR network for more than one week, the device **must be** taken to their IMO/IASO before connecting it back to the network. **KEEP THE COMPUTER CONNECTED TO THE NETWORK WHEN AT HOME STATION!**

c. **UNAUTHORIZED USAGE**: Use of commercial e-mail services, i.e., HOTMAIL, YAHOO, AOL etc. **is not authorized on government computers.** AKO e-mail services and their chatting rooms are the only authorized type of services for personal use on government computers. Downloading freeware or shareware **is not authorized** while using the government network. Your IASO/IMO/IAM must authorize any software the user may need to perform the job. **DO NOT DOWNLOAD UNATHORIZED PROGRAMS ON GOVERNMENT COMPUTERS!**

d. **PROHIBITED WEBSITES**. Users will not visit any website dealing with pornography, or any other sites that promulgates hate, or racial discrimination. Even though USAREUR have a program in place (WEBSENSE) to block these types of websites, there is always the possibility of new sites not yet caught up this program and others systems in place. **THE USER DOES NOT WANT TO BE THE SUBJECT OF AN INVESTIGATION!**

e. **SENSITIVE INFORMATION**. All sensitive but classified information must be sent via secure media. Secure media ranges from encrypted e-mail (PKI) to using approved classified systems i.e., computers, secure fax etc. Your IMO/IASO can provide guidance on acquiring PKI enabling to include Host Nation users that may require to process sensitive information on a regular basis due to the nature of their duties. **ALL MILITARY AND DOD CIVILIANS MUST BE PKI CERTIFIED!**

5. USER TRAINING AND AGREEMENT: All personnel requiring access to the Army Network must complete the DoD Annual Information Assurance Training. This training must be taken annually. Users will receive notification via e-mail when to re-take the training. Failure to complete the annual training may cause your network account to be disabled. Users must also read and sign an Acceptable User Policy agreement. The training and the agreement can be at the following website https://itt.eur.army.mil. First time users must request an account prior to taking the training.

6. **Reminder**. Army Regulation 25-2, Information Assurance, is punitive in nature and empowers a Commander to enforce disciplinary actions against violators of paragraph 4.a through 4.e of this memorandum. Military personnel are subject to UCMJ and Civilian punishment can range from administrative sanctions to loosing a job. **PROTECT YOU JOB/POSITION BY AVOIDING BECOMING A SUBJECT OF THIS TYPE OF INVESTIGATION!**

7. The POC for this memorandum is the Information Assurance Manager at DSN: 634-8222.

ERIK O. DAIGA
COL, MI
Commanding

DISTRIBUTION:
A